

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

300 N. South Street Lot 8, New Vienna, Ohio 45159
[INCLUDING ALL OUTBUILDINGS AND CURTILAGE]

Case No. **1:20-MJ-00481**

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the SOUTHERN District of OHIO, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

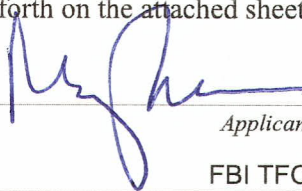
The search is related to a violation of:

| Code Section | Offense Description |
|--------------|--------------------------------------------------------------------------------------|
| 18: 2252 | Certain Activities Relating to Material Involving the Sexual Exploitation of Minors |
| 18: 2252A | Certain Activities Relating to Material Constituting or Containing Child Pornography |

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



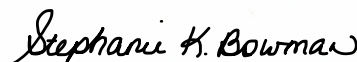
Applicant's signature

FBI TFO Mary Braun

Printed name and title

Sworn to before me and signed in my presence via electronic means.

Date: Jul 8, 2020



Judge's signature

City and state: CINCINNATI, OHIO

HONORABLE STEPHANIE K BOWMAN, Magistrate Judge

Printed name and title



ATTACHMENT A
DESCRIPTION OF PLACE TO BE SEARCHED

The address 300 N. South Street Lot 8, New Vienna, Ohio 45159 is a single family mobile home with beige siding and gray shutters. The front door is white in color. There is a black light post next to the driveway with the number 08 clearly visible. There is a detached wooden shed near the back door. (See photographs below)





ATTACHMENT B
LIST OF ITEMS TO BE SEIZED

The terms "child pornography" and "visual depictions," as used herein, have the same definitions listed in Section III of the attached affidavit, and those definitions are incorporated herein by reference.

1. Computer(s), computer hardware (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives, diskettes, and other memory storage devices), computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs, including, but not limited to, P2P software.
3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography, or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct.
4. In any format or medium, all child pornography or child erotica.
5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of the computer, or by other means for the purpose of distributing or receiving child pornography, or visual depictions.
6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through

interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by computer, any child pornography or any visual depictions.

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography or visual depictions.
8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography, or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.
9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.
10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.
11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.
12. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.
13. Any and all cameras, film, videotapes or other photographic equipment.
14. Any and all visual depictions of minors in order to compare the images to known and identified minor victims of sexual exploitation.

15. Any and all address books, mailing lists, supplier lists, mailing address labels, and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography or any visual depictions.
16. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.
17. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.
18. Any evidence of the presence or use of dropbox or peer-to-peer file sharing programs.

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO**

| | | |
|------------------------------------------------------------------------------------------|---|--------------------------------|
| In the Matter of the Search of: |) | No. 1:20-MJ-00481 |
| |) | |
| The residence located at 300 N. South Street Lot 8 New Vienna, Ohio 45159 |) | Magistrate Judge Bowman |
| |) | |
| | | UNDER SEAL |

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Mary P. Braun, a Detective with the Cincinnati Police Department and a Task Force Officer with the Federal Bureau of Investigation (FBI), being first duly sworn, hereby depose and state as follows:

I. EDUCATION TRAINING AND EXPERIENCE

1. I have been employed as a Police Specialist with the Cincinnati Police Department since 2004, and for the past ten years have been assigned to the Regional Electronics Computer Investigations (RECI) Task Force working on crimes involving computers and computer based crimes against children and others. Through my work in the Cincinnati Police Department, I have become familiar with the methods and schemes employed by persons who trade and collect child pornography as well as the manner in which adults seduce children for hands-on offenses. As a Task Force Officer, I have investigated federal criminal violations involving crimes against children, child pornography, and human trafficking. I have received formal training in the investigation of these matters at the Cincinnati Police Academy, the Federal Bureau of Investigation, and the National Center for Missing and Exploited Children, through other in-service training, and through private industry. As part of the Federal Bureau of Investigation's Violent Crimes Against Children/Child Exploitation Task Force, in 2011, I was deputized by the United States Marshals Service as a Special Deputy United States Marshal, thereby authorized to

seek and execute arrest and search warrants supporting a federal task force.

2. During my career as a Detective and Task Force Officer, I have participated in various investigations involving computer-related offenses and executed numerous search warrants to include those involving searches and seizures of computers, computer equipment, software, and electronically stored information. I have received both formal and informal training in the detection and investigation of computer-related offenses. As part of my duties as a Task Force Officer, I investigate criminal violations relating to child exploitation and child pornography including the illegal distribution, transmission, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2252(a) and 2252A.

3. As a Task Force Officer, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

II. PURPOSE OF THE AFFIDAVIT

4. The facts set forth below are based upon my own personal observations, investigative reports, and information provided to me by other law enforcement agents. I have not included in this affidavit all information known by me relating to the investigation. I have set forth facts to establish probable cause for a search warrant for the residential property located at 300 N. South Street Lot 8, New Vienna, Ohio 45159 (the SUBJECT PREMISES). I have not withheld any evidence or information which would negate probable cause.

5. The SUBJECT PREMISES to be searched is more particularly described in Attachment A, for the items specified in Attachment B, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2252 and 2252A the distribution, transmission, receipt, and/or possession of child pornography. I am requesting authority to search the entire SUBJECT PREMISES, including the residential dwelling, all outbuildings and any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

III. APPLICABLE STATUTES

6. Title 18, United States Code § 2252 makes it a crime to knowingly transport, ship, receive, distribute, sell or possess in interstate commerce any visual depiction involving the use of a minor engaging in sexually explicit conduct. For purposes of this statute, the term sexually explicit conduct is defined in 18 U.S.C. § 2256(2) as:

A. actual or simulated

- i. sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;
- ii. bestiality;
- iii. masturbation;
- iv. sadistic or masochistic abuse; or
- v. lascivious exhibition of the genitals or pubic area of any person.”

7. Title 18, United States Code § 2252A makes it a crime to knowingly mail, transport, ship, receive, distribute, reproduce for distribution, sell or possess child pornography in interstate commerce. It also makes it a crime to advertise, distribute or solicit in interstate commerce any material that reflects the belief or is intended to cause another to believe that the material contains an obscene visual depiction of a minor engaging in sexually explicit conduct or a visual depiction of an actual minor engaging in sexually explicit conduct. For purposes of this statute, the term child pornography is defined in 18 U.S.C. § 2256(8) as any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

- A. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
- B. such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
- C. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. The term sexually explicit conduct has the same meaning as in 18 U.S.C. § 2252, except for the subsection (B) definition of child pornography where it means:

- i. graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited;
- ii. graphic or lascivious simulated; (I) bestiality; (II) masturbation; (III) sadistic or masochistic abuse; or
- iii. graphic or simulated lascivious exhibition of the genitals or pubic area of any person.

8. Graphic, when used with respect to a depiction of sexually explicit conduct, means that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted. *See* 18 U.S.C. § 2256(10).

9. The following terms have the same meanings or explanations in both statutes:

- A. “minor” means any person under the age of eighteen years, pursuant to 18 U.S.C. § 2256(1);
- B. “visual depiction” includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image, pursuant to 18 U.S.C. § 2256(5);
- C. “computer” is defined in 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

IV. BACKGROUND REGARDING COMPUTERS, THE INTERNET, AND FILE SHARING PROGRAMS

10. Based on my knowledge, training, and experience, and the experience of other law enforcement officers, I have knowledge of the Internet and how it operates. I know that the Internet is a collection of computers and computer networks that are connected to one another via high-speed data links and telephone lines for the purpose of communicating and sharing data and information. Connections between Internet computers exist across state and international borders; therefore, information sent between two computers connected to the Internet frequently cross state

and international borders even when the two computers are located in the same state. The following paragraphs describe some of the functions and features of the Internet as it relates to the subject of this search warrant.

11. A website is a collection of Internet pages that Internet users can view. The web address is the name given to a website that enables Internet users to find the website. When a user types in the web address while connected to the Internet, the user will be connected to that website.

12. Many individuals and businesses obtain access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs servers; remotely store electronic files on their customer's behalf; and may provide other services unique to each particular ISP.

13. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. Those records often include identifying and billing information, account access information in the form of log-in files, e-mail transaction information, posting information, account application information, and other information both in computer data and written record format.

14. An Internet Protocol address (or simply "IP" address) is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned a unique IP address so that Internet traffic sent from and directed to that computer may be properly directed from its source to its destination. Most ISPs control a range of IP addresses.

15. When a customer logs into the Internet using the service of an ISP, the ISP assigns the computer used by the customer an IP address. The customer's computer retains that IP address for the duration of that session (i.e., until the user disconnects), and the IP address cannot be assigned to another user during that period. When an Internet user wishes to visit a website and types the

web address into his computer (e.g., www.cnn.com), that website receives a request for information from that customer's assigned IP address and sends the data to that IP address, thus giving the Internet user access to the website.

16. Computers are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including GIF (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.

17. Computers are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.

18. A computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 100 gigabytes are not uncommon. These drives can store tens of thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with

careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

V. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

19. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment.

This is almost always true because of the following:

- a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and
- b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

20. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child

pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

21. In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2252 and 2252A, and should all be seized as such.

VI. SEARCH METHODOLOGY TO BE EMPLOYED

22. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. Examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein;
- c. surveying various files, directories and the individual files they contain;
- d. opening files in order to determine their contents;
- e. scanning storage areas;
- f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or
- g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

23. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have

been deleted, they can be recovered months or years later using readily- available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

VII. INVESTIGATION AND PROBABLE CAUSE

24. In February 2019, your affiant received a CyberTip from the National Center for Missing and Exploited Children's (NCMEC) CyberTipline. NCMEC's CyberTipline is the nation's centralized reporting system for the online exploitation of children. The public and electronic service providers can make reports of suspected online enticement of children for sex acts, child pornography, child sex tourism, child sex trafficking and unsolicited obscene materials sent to a child. The electronic service provider in this case, Dropbox, Inc. reported that one of their users had uploaded 85 videos of suspected child pornography, beginning on October 10, 2018.

25. Dropbox, Inc. identified the user of the account as:

Screen/Username: Chris Brakefield

Email Address: chrisbrakefield@gmail.com

ESP User ID: 344977792

26. Your affiant reviewed the videos that were uploaded to Dropbox, Inc. The following is a description of several:

- a. (Falko) REP Video Part II (Part2-001).mp4 – A fifty second video in which a prepubescent female is laying on her stomach with her genital area exposed to the camera. An adult female's hands are seen rubbing the girl's genitals with a clear liquid. She then puts her finger inside the girl's anus.
- b. 6bbe48eaca957bfb3981cd52eb6efb34.mpg – A thirty-one second video in which a female toddler is performing oral sex on an adult male.
- c. 7.wmv – A one minute, eleven second video. A toddler aged female is naked from the waist down. An adult male is rubbing his penis on her vaginal area.
- d. CANGPJMM.mp4 – A 3 minute, 23 second movie in which a prepubescent female is laying on a bed, naked. An adult male is penetrating her vagina with his erect penis.
- e. MOV_0032.mp4 – This video is one minute and one second in length. A prepubescent male is laying on his back, naked. The camera is zoomed in on his penis. An adult male's penis comes into view. The adult ejaculates on the boy's penis.

27. A search warrant was sent to Dropbox, Inc. to get the contents of account User ID 344977792. The following user information was returned:

Name: Chris Brakefield

Email Address: chrisbrakefield@gmail.com

ESP User ID: 344977792

Joined: October 5, 2014

28. The results received from Dropbox, Inc. included 159 videos of child pornography.

Below are the descriptions of several:

- a. Tio.wmv – This is a 6 minute, 36 second video in which a toddler aged female is laying on a bed, naked with her legs spread, exposing her vagina. An adult male puts his penis on the outside of her vaginal area. He rubs his penis on her until he ejaculates. The man sits the girl up and puts his penis in her mouth. He then lays her on her stomach and rubs his penis on her anus.
- b. IMG_3867.mov – This video is 1 minute, 24 seconds in length. An adult puts his penis in the mouth of a prepubescent girl. The girl is blindfolded. At the end of the video the girl begins to cry. The man is heard saying, “Was that too hard?”.
- c. CANGPJMM.mp4 – This video is 3 minutes, 23 seconds in length. There is a naked prepubescent girl laying on a bed while an adult male penetrates her vagina with his erect penis.
- d. pthc jenny mama suck 9yo.avi – This 1 minute 18 second video shows a prepubescent female performing oral sex on an adult’s penis.
- e. Baby-J_3.mp4 – This is a 2 minute, 20-second-long video in which an adult man puts his penis into the vagina of a prepubescent girl. He ejaculates on her stomach.
- f. MOV_0032.mp4 – This video is one minute and one second in length. A prepubescent male is laying on his back, naked. The camera is zoomed in on his penis. An adult male’s penis comes into view. The adult ejaculates on the boy’s penis.

29. Included in the results were several dates of Authentication Information, where the user would need to put the email address and password to enter the Dropbox, Inc account. One of those dates was April 5, 2018. After the account was logged into, 220 files with names indicative

of child pornography were uploaded. Dropbox was unable to provide any IP information associated with the account but according to Dropbox's user guide they do require email accounts associated with accounts be verified in order to use some features and post on their forums.

30. A Federal Grand Jury Subpoena was served to Google to get the account information and IP address history for the email account chrisbrakefield@gmail.com. Google returned the following Subscriber Information:

Name: Chris Brakefield

Email: chrisbrakefield@gmail.com

Recovery Email: chrisbrakefield84@yahoo.com

Created on: 01/19/2010

SMS: +17405054590

31. Google returned the following IP addresses as ones used by the target email account between October 3, 2018 and April 19, 2019:

2607:fcc8:8dce:f400:654b:41c4:92bb:4953

2607:fcc8:8dce:f400:e07d:b172:b45b:fc56

2607:fcc8:8dce:f400:c560:eb53:2379:5a2

2607:fcc8:8dce:f400:d043:5a90:9d9d:489a

2607:fcc8:8dce:f400:c8f8:96b1:2c7e:381a

2607:fcc8:8dce:f400:19e9:2d83:3be7:d932

2607:fcc8:8dce:f400:8996:8f71:d7bd:7a8f

2607:fcc8:8dce:f400:65f0:3a94:9e82:eb4c

2607:fcc8:8dce:f400:1de9:f1d5:e432:494c

2607:fcc8:8dce:f400:9132:fb37:bad4:ee45

2607:fcc8:8dce:f400:3449:207a:abf5:59ff

2607:fcc8:8dce:f400:48a9:7e39:4ba1:29ce

2607:fcc8:8dce:f400:a4db:1828:4097:7516

2607:fcc8:8dce:f400:616b:74a6:c2e8:69f9

2607:fcc8:8dce:f400:a1cf:f2f4:63e6:e664

2607:fcc8:8dce:f400:d481:c39:cf9e:cdb0

2607:fcc8:8dce:f400:fd3f:b099:971b:f887

2607:fcc8:8dce:f400:10d1:faaf:42e9:60b3

2607:fcc8:8dce:f400:2c96:61af:7d27:fc8c

32. All of the IP addresses resolved to Charter Communications. A Federal Grand Jury Subpoena was sent, requesting the subscriber information.

33. Charter Communications returned the subscriber information for the IP addresses. The information provided on the IP addresses is as follows:

Subscriber Name: Chris Brakefield

Subscriber Address: 300 N. South Street Lot 8, New Vienna, Ohio 45159

Username/Email: chrisbrakefield@gmail.com

Phone Number: (740)505-4590

34. A search for “Chris Brakefield” on several law enforcement search engines and Ohio Bureau of Motor Vehicle website, found a listed address for Christopher L. Brakefield as 300 N. South Street Lot 8, New Vienna, Ohio 45159, Date of Birth 0XX/XX/1984, Social Security Number XXX-XX-8812.

35. On July 30, 2019 at approximately 9:00 A.M, your affiant went to the SUBJECT PREMISES and observed the house. The light post in front of the house had the numbers 08 on it. Your affiant also observed one vehicle in the driveway. The vehicle had Ohio license tags FWP7689. Your affiant observed two people exiting the vehicle. A man matching the description of Chris Brakefield was seen getting out of the passenger side of the car. The woman exiting the driver’s side was later identified as Melissa Brakefield (Date of Birth XX/XX/1981,

Social Security Number XXX-XX-7017), the owner of the car. Melissa Brakefield's Ohio Driver's License lists the SUBJECT PREMISES as her address. The vehicle is registered to that address as well.

36. Your affiant again went to the SUBJECT PREMISES on June 30, 2020. There was one vehicle in the driveway, with Ohio license tag FWP7689. That vehicle is still registered to Melissa Brakefield and the SUBJECT PREMISES. Additionally, Christopher Brakefield's latest Ohio Identification Card lists the SUBJECT PREMISES as his home address.

VIII. CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

37. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

- A. Those who receive and may be collecting child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- B. Those who receive and may be collecting child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- C. Those who receive and may be collecting child pornography often times possess and maintain any "hard copies" of child pornographic material that may exist – that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and video tapes for many years.

- D. Likewise, those who receive and may be collecting child pornography often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.
- E. Those who receive and may be collecting child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- F. Those who receive and may be collecting child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography offenders throughout the world.
- G. When images and videos of child pornography are stored on computers and related digital media, forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.

38. Based upon the conduct of individuals involved in the collection of child pornography set forth in the above paragraph, namely, that they tend to maintain their collections at a secure, private location for long periods of time, and that forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media, there is probable cause to believe that evidence of the offenses of receiving and possessing child pornography is currently located at the SUBJECT PREMISES.

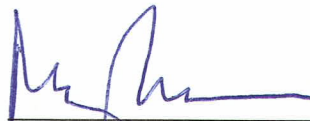
IX. CONCLUSION

39. Based on the aforementioned factual information, your affiant submits there is probable cause to believe that a resident of 300 N. South Street Lot 8, New Vienna, Ohio 45159 is a collector of child pornography, that violations of Title 18, United States Code, §§ 2252 and 2252A have been committed, and evidence of those violations is located in the premises described

in Attachment A. Your affiant respectfully requests that the Court issue a search warrant authorizing the search and seizure of the items described in Attachment B.

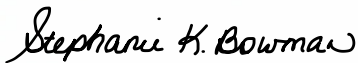
REQUEST FOR SEALING

40. It is further respectfully requested that this Court issue an Order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the requisite inventory notice. Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and premature disclosure of the contents of this affidavit and related documents may have a negative impact on this continuing investigation and may jeopardize its effectiveness



Mary P. Braun
Detective/TFO
Cincinnati Police Department/FBI

Sworn to and subscribed before me this 8th day of July 2020, via electronic means.



HON. STEPHANIE K. BOWMAN
United States Magistrate Judge
Southern District of Ohio



ATTACHMENT A
DESCRIPTION OF PLACE TO BE SEARCHED

The address 300 N. South Street Lot 8, New Vienna, Ohio 45159 is a single family mobile home with beige siding and gray shutters. The front door is white in color. There is a black light post next to the driveway with the number 08 clearly visible. There is a detached wooden shed near the back door. (See photographs below)





ATTACHMENT B
LIST OF ITEMS TO BE SEIZED

The terms "child pornography" and "visual depictions," as used herein, have the same definitions listed in Section III of the attached affidavit, and those definitions are incorporated herein by reference.

1. Computer(s), computer hardware (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives, diskettes, and other memory storage devices), computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs, including, but not limited to, P2P software.
3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography, or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct.
4. In any format or medium, all child pornography or child erotica.
5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of the computer, or by other means for the purpose of distributing or receiving child pornography, or visual depictions.
6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through

interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by computer, any child pornography or any visual depictions.

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography or visual depictions.
8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography, or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.
9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.
10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.
11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.
12. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.
13. Any and all cameras, film, videotapes or other photographic equipment.
14. Any and all visual depictions of minors in order to compare the images to known and identified minor victims of sexual exploitation.

15. Any and all address books, mailing lists, supplier lists, mailing address labels, and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography or any visual depictions.
16. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.
17. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.
18. Any evidence of the presence or use of dropbox or peer-to-peer file sharing programs.

interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by computer, any child pornography or any visual depictions.

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography or visual depictions.
8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography, or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.
9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.
10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.
11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.
12. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.
13. Any and all cameras, film, videotapes or other photographic equipment.
14. Any and all visual depictions of minors in order to compare the images to known and identified minor victims of sexual exploitation.

15. Any and all address books, mailing lists, supplier lists, mailing address labels, and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography or any visual depictions.
16. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.
17. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.
18. Any evidence of the presence or use of dropbox or peer-to-peer file sharing programs.